

Compliance-Management-Systeme

Bay / Hastenrath

4. Auflage 2026
ISBN 978-3-406-81849-3
C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen. beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

dem Kapitalmarkt-, Sozialversicherungs- und Datenschutzrecht ergeben. Eine rechtliche Fallbegleitung ist daher zwingend.¹²⁷

Der Datenschutz stellt hohe Anforderungen an die Begründbarkeit und Dokumentation 178 der Maßnahmen. Daher sollte der Datenschutzbeauftragte frühzeitig in entsprechende Fragestellungen iRd Untersuchung eingebunden und die Abwägungen dokumentiert werden. IdR kommt es iRv Untersuchungshandlungen zur Verarbeitung personenbezogener Daten,¹²⁸ häufig zu rechtfertigen mit dem berechtigten Interesse des Arbeitgebers¹²⁹. Werden personenbezogene Daten für eine Untersuchung genutzt, entspricht das nicht mehr ihrem ursprünglichen Verwendungszweck. Der Betroffene ist über die Zweckänderung zu informieren¹³⁰ und kann wiederum Auskunftsansprüche¹³¹ geltend machen.¹³² Da sich die datenschutzrechtlichen Fristen am Zweck der Verwendung, Art und Ablageort der Daten ausrichten, sollten vorab sinnvolle Kategorien gebildet und mit dem Datenschutzbeauftragten abgestimmt werden, um im Ernstfall eine zügige Prüfung und Maßnahmenergreifung zu ermöglichen. Nach Abschluss des Falles muss geprüft werden, welche Daten zu löschen und wer über die Untersuchung zu informieren ist. Die Tätigkeiten sollten in einem Regelwerk zusammengefasst werden.

Das Betriebsverfassungsrecht bestimmt maßgeblich über die Ausgestaltung und Grenzen 179 einer Untersuchung, insbes. in Bezug auf gesetzliche Überwachungspflichten¹³³ und das Mitbestimmungsrecht bei technischen Überwachungseinrichtungen¹³⁴. Die Mitbestimmungsrechte zu technischen Systemen reichen vom Einsatz der Software bis hin zu Zugriffs- und Auswertungsrechten. Daher empfiehlt es sich, vorab eine grundsätzliche Betriebsvereinbarung mit entsprechenden Mitwirkungs- und Informationsrechten zu vereinbaren. Die Absprache von Verhaltensregeln für eine Sonderuntersuchung ist ein wichtiger Baustein für eine vertrauensvolle Zusammenarbeit zwischen Arbeitgeber und Arbeitnehmervertretung und sollte ohne Zeitdruck durch eine konkrete Untersuchung erfolgen.

Eine anlassbezogene Sonderuntersuchung ist eine heikle Situation für den Betroffenen. 180 Mit der Untersuchung stehen sein Ruf, sein Arbeitsplatz und eventuell sogar seine Freiheit auf dem Spiel. Gleichzeitig besteht die Möglichkeit, dass sich der Verdacht in der Untersuchung nicht erhärtet oder es sich gar um eine gezielte Verleumdung handelt. Dann dürfen dem Betroffenen keine Nachteile aus der Untersuchung erwachsen, in letzterem Fall sollte im Anschluss die Verleumdung untersucht werden. Eine Sonderuntersuchung verlangt nach hoher Professionalität aller Beteiligten und der strikten Beachtung der Persönlichkeitsrechte des Betroffenen, denn jeder Betroffene hat das Recht auf eine faire Behandlung. Fairness bedeutet in diesem Zusammenhang, dass der Untersuchungsgegenstand klar definiert ist und die Untersuchung selbst objektiv und professionell durchgeführt wird. Dies schließt die Wahrung der Vertraulichkeit (striktes „need-to-know“-Prinzip) aller Handlungen und Beteiligter mit ein. Das Ziel der Sonderuntersuchung ist es nicht, den Betroffenen im finalen Verhör durch entsprechenden Druck zu „knacken“ und zu einem Geständnis zu bewegen wie in einer US-amerikanischen Krimiserie, sondern den Tathergang möglichst eindeutig zu rekonstruieren und mit Beweisen zu untermauern. Es bedarf als Untersuchender einer neutralen und vorurteilsfreien Haltung (Unschuldsvermutung), da sowohl belastende als auch entlastende Fakten erhoben werden müssen. Auch muss sich der Betroffene strafrechtlich nicht selbst belasten.

¹²⁷ DICO S 04 – Interne Untersuchungen, 2019, S. 10 f.

¹²⁸ ISd Art. 4 Nr. 1 DS-GVO; zu bedenken sind auch die strengen Anforderungen an die Übermittlung personenbezogener Daten an Dritte innerhalb und außerhalb der EU.

¹²⁹ Art. 6 Abs. 1 Buchst. f. DS-GVO.

¹³⁰ Art. 13 Abs. 3; DS-GVO Art. 14 Abs. 4 DS-GVO.

¹³¹ Art. 15 DS-GVO.

¹³² Zur Abwägung DICO S 04 – Interne Untersuchungen, 2019, S. 11 ff.

¹³³ § 80 Abs. 1 Nr. 1 BetrVG.

¹³⁴ § 87 Abs. 1 Nr. 6 BetrVG.

- 181** Mitarbeiter, die Sonderuntersuchungen durchführen, unterliegen einem engen rechtlichen Möglichkeitsrahmen aus verschiedenen Gesetzen. Gleichwohl fehlt derzeit ein rechtlich definierter Handlungsrahmen für die Durchführung von Sonderuntersuchungen.¹³⁵ Die komplexe Rechtslage bringt ermittelnde Mitarbeiter in die Gefahr, selbst Gesetze zu verletzen und sich strafbar zu machen. Dies würde die Beweisverwertung vor Gericht gefährden. Ermittler sollten daher regelmäßig zu allen relevanten Aspekten einer Sonderuntersuchung geschult und bedarfsweise Fachexperten hinzugezogen werden.

2. Sonderuntersuchung (Internal Investigation)

a) Hinweis geht ein

- 182** Hinweise auf einen möglichen Compliance-Verstoß können einerseits aus dem Hinweisgeberverfahren (→ Rn. 136–158), aus Erkenntnissen aus vorangegangenen Prüfungen von Compliance (→ Rn. 168–170), der Internen Revision oder anderen prüfenden Einheiten sowie Anfragen von Behörden¹³⁶ stammen. Die Vielfalt potenzieller Sachverhalte ist groß: Neben allgemeinen Pflichtverletzungen können auch Bestechung, Korruption und Untreue, Verstöße gegen das Datenschutzrecht, Kartellrecht, Produktsicherheitsrecht, Sozialversicherungsrecht, Subventionsrecht, Umweltrecht etc zu untersuchen sein. Ein im Jahr 2022 erhobenes Meinungsbild weist folgenden Themen eine besonders hohe Relevanz für künftige Sonderuntersuchungen zu: Cybercrime, ESG (Environmental, Social & Governance, inkl. Menschenrechte), Personalthemen (Mobbing, #meetoo, Code of Conduct) sowie die Aufklärung von Datenschutzverstößen.¹³⁷
- 183** Geht der Hinweis nicht auf Erkenntnisse interner Voruntersuchungen zurück, ist die Meldung zunächst zu plausibilisieren. Mit dem erhärteten Anfangsverdacht wird die Sonderprüfung eingeleitet. Sofern die Gefahr einer weiteren Schädigung besteht oder Spuren beseitigt werden könnten, sollten ad-hoc Maßnahmen zur Sicherung erwogen werden wie bspw. die Freistellung des Betroffenen, Sperrung von Zugang und Zugriffen sowie der Entzug von Vollmachten. Der aktuelle Kenntnisstand kann – je nach Sachverhalt einerseits und Ausgestaltung des Reportings andererseits – bereits ein ad-hoc-Reporting an die Unternehmensleitung oder den Aufsichtsrat auslösen. Vorwürfe gegen Organmitglieder, strafrechtliche Relevanz des Sachverhalts oder definierte Wertgrenzen sollten zur sofortigen Information der Unternehmensleitung und/oder des Aufsichtsrats führen. Sollte sich der Hinweis auf ein Organmitglied, die Compliance-Funktion oder aufklärende Einheiten beziehen, muss sichergestellt werden, dass die Aufklärung objektiv und frei von Interessenkonflikten erfolgen kann. Es empfiehlt sich eine externe Unterstützung vorzubereiten.

b) Planung der Untersuchung

- 184** Die Ressourcenplanung ist abhängig vom Sachverhalt. Die Verfügbarkeit sachkundiger Ermittlungsteams ist essenziell, weshalb bei Bedarf über eine externe Unterstützung entschieden werden muss. Wird eine externe Unterstützung erwogen, müssen die Beauftragung selbst sowie die Bereitstellung eines entsprechenden Budgets kurzfristig erfolgen. Die technische Ausstattung und Systemzugänge sind bereitzustellen.
- 185** Verfügt das Unternehmen über kein dediziertes Ermittlerteam, bieten sich Mitarbeiter der Rechts- oder Compliance-Abteilung sowie der Internen Revision an (ähnlich der Überlegung zu Compliance-Audits → Rn. 160–166). Je nach Sachverhalt werden interne und externe Experten wie Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, IT-Spezialisten,

¹³⁵ Zur detaillierten Darstellung s. Naber/Ahrens CCZ 2020, 36.

¹³⁶ In einer Befragung gaben 50 % der Unternehmen an, dass sie Sonderuntersuchungen aufgrund von Behördenanfragen gestartet haben. Details s. DICO, Interne Untersuchungen in Deutschland – 2022, S. 27.

¹³⁷ DICO, Interne Untersuchungen in Deutschland – 2022, S. 10, 68 f.

Forensiker hinzugezogen. Zeichnet sich ab, dass eine gerichtliche Würdigung des Falles möglich sein könnte, bspw. aufgrund der gehobenen Stellung des Betroffenen, der strafrechtlichen Relevanz der Tat oder der Schadenshöhe, sollte eine fachkundige externe Unterstützung für die sichere Gerichtsverwertbarkeit der Beweise hinzugezogen werden. Dies sollte vor Eintritt eines Ernstfalls vorbereitet werden.

c) Durchführung der Sonderuntersuchung

Je nach Sachverhalt bieten sich verschiedene Untersuchungsmethoden an:¹³⁸ Hintergrundrecherchen (zur Aufdeckung möglicher Beziehungsgeflechte), Interviews mit Informations-trägern und Betroffenen, Datenanalysen (strukturierte Daten), Durchsicht von physischen Unterlagen sowie Analyse elektronischer Unterlagen (unstrukturierte Daten, eDiscovery).

Interviews sind eine übliche und gleichzeitig sensible Methode aufgrund der Anforderungsdichte an die Durchführung. Es muss vorab geklärt werden, ob der Betroffene freiwillig teilnimmt oder eine Pflicht zur Teilnahme besteht¹³⁹, inwieweit eine Pflicht zur Aussage trotz Selbstbelastungsverbot besteht, ob und in welcher Besetzung ein Rechtsbeistand hinzugezogen werden soll und welche Mitbestimmungs- und Informationsrechte der Betriebsrat inne hat. Ein Interview folgt keiner amerikanischen Krimiserie, sondern dient der Faktensammlung. Ein professioneller und kollegialer Umgang ist zu wahren, von Suggestivfragen, gezielter Beeinflussung oder anderen Methoden zum Druckaufbau ist abzusehen.

Sollen iRd eDiscovery bspw. E-Mails, Kalendereinträge und Chat-Nachrichten ausgewertet werden, sind die Grenzen aus datenschutzrechtlichen Vorgaben, Betriebsvereinbarungen und Mitbestimmungsrechten zu beachten. Wird die private Nutzung von E-Mails etc. erlaubt oder geduldet, kann dies die Untersuchungsmöglichkeiten ebenfalls begrenzen.

Die Sonderuntersuchung ist durchgängig sorgfältig zu dokumentieren, Maßstab ist die spätere Gerichtsverwertbarkeit der Dokumentation. Hat die Sonderuntersuchung eine potenziell strafbare Handlung zum Gegenstand, kann nicht ausgeschlossen werden, dass Ermittlungsbehörden (Polizei und Staatsanwaltschaft) Unterlagen für eigene Untersuchungen beschlagnahmen. Damit kann das Unternehmen die dem Betroffenen zugesicherte Vertraulichkeit nicht sicher aufrechterhalten.¹⁴⁰

II. Sanktionen

Wurden in der Sonderuntersuchung Rechtsverstöße festgestellt, ist die Unternehmensleitung verpflichtet, Sanktionen zu ergreifen. Ihre Ausgestaltung ist Ermessenssache – muss aber angemessen sein. Für die Beurteilung der Angemessenheit sind verschiedene Aspekte abzuwägen wie die Schwere der Tat selbst (Qualität des Regelverstosses, Häufigkeit des Fehlverhaltens, entstandener Schaden, Konsequenzen für das Unternehmen, Abschreckung von Nachahmungstätern etc), das Verhalten des Betroffenen (Gründe für das Fehlverhalten, Kooperationsbereitschaft in der Aufklärung, Einsicht), Sichtbarkeit der Tat und damit Notwendigkeit sichtbarer Reaktionen innerhalb und außerhalb des Unternehmens (behördliche Ermittlungen, Presseberichterstattung, Reaktionen von Geschäftspartnern etc).

Das Unternehmen kann Sanktionen aus einem umfangreichen Wirkungsspektrum ergreifen: Ermahnung, Abmahnung, ordentliche oder außerordentliche Kündigung sowie Strafanzeige. Daneben sind Optionen der Vermögensrückführung abzuwägen wie die

¹³⁸ Eine Aufstellung der Beliebtheit der eingesetzten Methoden s. KPMG, Wirtschaftskriminalität in Deutschland, 2023, S. 35.

¹³⁹ Mitarbeiter sind durch arbeitsvertragliche Pflichten nach §§ 666, 675 BGB zur Auskunft und Mitwirkung verpflichtet.

¹⁴⁰ Einen Überblick zur Diskussion um das Beschlagnahmeverbot nach § 97 Abs. 1 StPO, § 160a StPO gibt Bürkle Compliance/Lescher § 15 Rn. 101, Ansätze zur Überprüfung des eigenen Vorgehens liefern das U. S. Department of Justice, Criminal Division Evaluation of Corporate Compliance Programs, 2024, Kap. III.B., S. 19f.

Geltendmachung von zivilrechtlichen Schadensersatzansprüchen oder die Einholung eines notariellen Schuldanerkenntnisses. Besteht eine D&O oder Vertrauensschadenversicherung, sollte die Inanspruchnahme für den Fall erwogen werden. Die Sanktion von Mitarbeitern löst ebenfalls Mitbestimmungsrechte aus, weshalb der Betriebsrat entsprechend einzubeziehen ist. Kommt es zu behördlichen Ermittlungen, drohen Geld- und Haftstrafen nach Strafgesetzbuch und Ordnungswidrigkeitengesetz.

- 192 Die ergriffenen Sanktionen haben einen starken Einfluss auf die Glaubwürdigkeit des CMS und die Compliance-Kultur. Sowohl die Untersuchung selbst als auch die Sanktionen sollten frei von Bevorzugung sein und unabhängig von Hierarchieebene, Rolle, Netzwerkzugehörigkeit etc. erfolgen.¹⁴¹
- 193 Non-Compliance lässt sich nicht vollständig verhindern, der Umgang mit der Thematik wirkt jedoch intern und extern. Studien zeigen, dass über 90 % der befragten Unternehmen ihr eigenes Verhalten in der Geschäftsbeziehung verändern, wenn ihr Partner einen Fall von non-Compliance erlebt hat. Knapp die Hälfte der Unternehmen (44 %) schärft Vertragsbedingungen nach oder ist bereit, die Geschäftsbeziehungen abubrechen (49 %). Wesentlich für die Weiterführung der Vertragsbeziehung ist die unabhängige Sachverhaltsaufklärung (83 %), die Einführung eines CMS und die Entlassung des Täters (74 %). Zunehmend wichtiger wird die Tatsache, dass die Staatsanwaltschaft die Ermittlungen beendet hat (67 %).¹⁴²

III. Prozesse und Kontrollen

- 194 IRd Sonderuntersuchung ergeben sich aus dem Tathergang selbst oder iRd Aufklärung regelmäßige Hinweise auf potenzielle Schwächen in Prozessen und Kontrollen. Auf Basis einer Ursachenanalyse (Root Cause Analysis) wird nun nach den tatsächlichen Schwächen gesucht, die zum Fehlverhalten geführt haben. Diese Ursachen werden analysiert und behoben oder kompensiert, um künftiges Fehlverhalten zu vermeiden. In diesem Schritt geht es nicht um das „Wer“, sondern um das „Warum“ der Tat.¹⁴³ Diese wertvollen Erkenntnisse können dann in die Verbesserung des Internen Kontrollsystems (→ Rn. 114–118) und des CMS eingebracht werden und liefern damit einen wesentlichen Beitrag zur Weiterentwicklung des CMS.
- 195 Neben der Verbesserung der Kontrollumgebung werden idR auch die Prozesse verbessert. Zu den üblichen Maßnahmen gehören die Verbesserung des Hinweisgeberverfahrens und Etablierung von Eskalationsprozessen (→ Rn. 136–159), regelmäßige Prüfungen der Wirksamkeit der ergriffenen Managementmaßnahmen, Richtlinien zum Umgang mit Risiken in der Lieferkette (→ Rn. 58–62, → Rn. 65–95), initiale Risikoanalyse (→ Rn. 13 f.), Sensibilisierungsschulungen (→ Rn. 106–111).¹⁴⁴

E. Fazit

- 196 Das CMS kann mit einem Bücherregal verglichen werden, welches ein organisatorisches Framework für die iRd Ausgestaltung des Compliance-Programms identifizierten risikoexponierten Fachthemen, die als Bücher eingebracht werden, bildet. Auf Basis der Risikoanalyse wird entschieden, welches Thema eines eigenständigen Buchs bzw. Programms bedarf. Die Programme sollten risikobasiert gestaltet werden, indem solche mitigierenden

¹⁴¹ S. auch die Fragen zum Konsequenzen-Management in U.S. Department of Justice, Criminal Division Evaluation of Corporate Compliance Programs, 2024, Kap. II. C., S. 14–16.

¹⁴² KPMG, Wirtschaftskriminalität in Deutschland 2023: Gegen jede Regel, S. 40 f.

¹⁴³ Einen guten Einstieg bietet die ‚5-Why‘-Methode, bei der jede Antwort mit einem weiteren ‚warum‘ vertieft wird, um zum eigentlichen Kern des Problems vorzustoßen.

¹⁴⁴ KPMG, Wirtschaftskriminalität in Deutschland 2023: Gegen jede Regel, S. 48.

Maßnahmen ergriffen werden, die auf das identifizierte, unternehmensindividuelle Risiko und die entsprechenden Risikoszenarien zugeschnitten sind. Die Programme müssen zwingend präventive, aufdeckende und reaktive Maßnahmen beinhalten. Sie selbst und die ergriffenen Maßnahmen bedürfen fortlaufenden Anpassung, um neue oder veränderte Anforderungen ebenso wie Erkenntnisse aus der eigenen Compliance-Arbeit angemessen zu reflektieren.

Ziel des Compliance-Programms ist es, rechtliche und reputationsbezogene Risiken zu 197
mitigieren, also im Ideal Compliance-Verstöße weitgehend zu verhindern oder mind.
frühzeitig zu erkennen und Prozessschwächen zu beheben. Schnell rückt das Verhalten der
Mitarbeiter in den Vordergrund. Neben den impliziten Regeln (Stichwort Kultur) und den
expliziten Regeln (Stichwort Regelwerk als Teil des Programms) stellt auch die Einbettung
des gewünschten Verhaltens in geeignete Prozesse ein wesentliches Präventionselement dar.
Erst indem die Regeleinhaltung durch aufdeckende Maßnahmen kontrolliert und im
Rahmen reaktiver Maßnahmen konkrete Vorfälle aufgeklärt, Fehlverhalten sanktioniert
und Prozesse verbessert werden, schließt sich der Kreis.

Der Erfolg des Compliance-Programms hängt maßgeblich davon ab, ob die Mitarbeiter 198
es aktiv unterstützen. Daher empfiehlt sich ein Perspektivwechsel: Regelungsdichte, Ver-
ständlichkeit und Auffindbarkeit von Regeln, Hürden für gewünschtes Verhalten und
Aufdeckungswahrscheinlichkeit von unerwünschtem Verhalten sollten im Fokus stehen –
oder kurz, es bedarf einer Machbarkeitsanalyse des eigenen Konzepts. Feedback durch
Kontrollen und Audits helfen, effektive Maßnahmen von weniger effektiven zu unterschei-
den und letztere weiterzuentwickeln oder aufzugeben.

Wo Menschen handeln, passieren Fehler und auch Verstöße, da selbst integre Menschen 199
manchmal falsche Entscheidungen treffen. Mit dem Compliance-Programm unterstützt die
Compliance-Funktion alle Mitarbeiter, Führungskräfte und Organe dabei, in ihrem Ar-
beitsalltag regelkonforme Entscheidungen zu treffen.

beck-shop.de
DIE FACHBUCHHANDLUNG



beck-shop.de
DIE FACHBUCHHANDLUNG

§ 5. Compliance-Organisation

Übersicht

	Rn.
A. Einleitung	1
B. Aufbau der Compliance-Organisation	6
I. Funktionen der Compliance-Organisation	7
1. House of Compliance	7
2. Regelkreis Compliance-Organisation	11
II. Zuordnung und Aufbau der Compliance-Organisation	25
1. Klassische Varianten der Zuordnung: Vor- und Nachteile	25
2. Alternativer Ansatz: Die integrierte Compliance-Organisation	30
3. Globale Compliance-Organisation	32
4. Berichtslinien	36
5. Rechte der Compliance-Officer	38
6. Schutz der Compliance-Officer	39
III. Auswahlkriterien für die Compliance Officer	40
1. Allgemeine Auswahlkriterien	40
2. Besonderheiten bei Compliance-Beauftragten in ausländischen Tochterge- sellschaften	43
IV. Regelungswerke für die Compliance-Organisation	48
1. Mission Statement	49
2. Satzung und Geschäftsordnung	51
3. Code of Conduct	52
4. Compliance-Richtlinie	55
C. Einführung und Weiterentwicklung der Compliance-Organisation	60
I. Praktische Hinweise für die Einführungsphase	61
1. Tone from the Top	61
2. Bedeutung der Regelungswerke	66
3. Schulung	68
4. Sichtbarkeit im Unternehmen in der Einführungsphase	69
5. Anpassungsbedarf im Ausland	70
6. Compliance-Erklärung	74
II. Fortentwicklung der Compliance-Organisation	75
1. Sichtbarkeit der Compliance-Organisation im Unternehmen	75
2. Aus- und Weiterbildung der Compliance-Officer	77
3. Incentive-Systeme für Compliance-Officer	80
4. Fortentwicklung der Kommunikationskanäle	81
5. Selbstauditierungsprogramme	84
6. Mock Audit	88
7. Digitalisierung der Compliance-Prozesse	91
D. Praxisbeispiele zu Hilfsmitteln und Mustern	93
I. Richtlinie Compliance – deutsche Fassung	93
II. Richtlinie Compliance – englische Fassung	94
III. Compliance-Erklärung (Statement of Compliance) – deutsche Fassung	95
IV. Compliance-Erklärung (Statement of Compliance) – englische Fassung	96
V. Fragebogen: Einführung Compliance für ausländische Tochtergesellschaften (englisch)	97
VI. Code of Conduct (Auszug) – deutsche Fassung	98
VII. Code of Conduct (Auszug) – englische Fassung	99
VIII. Fragebogen – Selbstauditierung für ausländische Tochtergesellschaften (eng- lisch)	100
IX. Ernennungsschreiben für einen Compliance-Officer – deutsche Fassung	101
X. Ernennungsschreiben für einen Compliance-Officer – englische Fassung	102

A. Einleitung

Die Einführung einer Compliance-Organisation hat idR eine Vorgeschichte. Im güns- 1
tigeren Fall sieht sich die Unternehmensleitung durch die allgemeine Diskussion zu dem
Thema Compliance veranlasst, eine Compliance-Organisation aufzubauen. Aber auch

unternehmensinterne Vorfälle bilden den Katalysator für die Einführung eines Compliance-Management-Systems, da die Unternehmensleitung erkannt hat, dass zum Schutz des Unternehmens zusätzliche Maßnahmen erforderlich sind. Mit der Einführung eines solchen Systems wird sodann entweder ein externer Berater oder typischerweise die Rechtsabteilung betraut, sofern eine solche vorhanden ist. Auch entscheiden sich viele Unternehmen mit zunehmender Tendenz, die Stelle eines Compliance-Officers zu besetzen. Andere Fälle, die eine eigene Compliance Organisation erfordern, sind etwa der Exit eines Startups oder die Ausgliederung von Unternehmensbestandteilen.¹ Auch wird iRd Know-Your-Customer Prüfung ab einem bestimmten Vertragsvolumen oder Vertragsbedeutung zunehmend von Lieferanten oder Vertriebspartnern eine eigene Compliance-Organisation verlangt.²

- 2 Die Vorgaben der Unternehmensleitung enthalten oft widerstreitende Interessen. Auf der einen Seite wird ein optimaler Schutz gewünscht. Dies soll allerdings ohne wesentliche zusätzliche Kosten, insbes. nur mit geringem **Headcount**, erreicht werden. Auch wird kein wesentlicher zusätzlicher Organisationsaufwand gewünscht: „Compliance soll die vorhandene Organisation nicht stören.“
- 3 Bei der sich anschließenden Einführung einer Compliance-Organisation sollte davon ausgegangen werden, dass viele Themen im Unternehmen bereits organisiert sind, bei denen Compliance eine Rolle spielt. So gibt es vielleicht schon eine Zollabteilung, eine Interne Revision oder die Rechtsabteilung. Alle diese Abteilungen haben sich auch bislang um Compliance gekümmert. Auch gibt es mitunter schon mehrere Personen, die Aufgaben erfüllen, die sich mit Compliance überschneiden, wie etwa Datenschutzbeauftragte, Informationssicherheitsbeauftragte (Chief Information Security Officer), Sicherheitsbeauftragte in der Arbeitssicherheit, Geldwäschebeauftragte, etc. Mit der Erkenntnis, dass Compliance eigenständig organisiert werden sollte, ergibt sich die Notwendigkeit, alle diese Funktionen in ein **einheitliches System** zu überführen und dafür eine Aufbauorganisation und eine Ablauforganisation festzulegen. Diese Vorgehensweise ist nicht neu. Ebenso wurden bspw. Qualitätssicherungssysteme eingeführt.
- 4 Der Aufbau der Compliance-Organisation richtet sich nach **verschiedenen Kriterien**.³ Zum einen sind die Unternehmensgröße – also Umsatz und Mitarbeiter – relevant sowie die Branche, in der das Unternehmen tätig ist. Auch spielt die Wertschöpfungstiefe eine erhebliche Rolle. Der Aufbau der Compliance-Organisation unterscheidet sich in Produktionsunternehmen deutlich von reinen Vertriebsunternehmen. Daneben ist zu berücksichtigen, inwieweit das Unternehmen international tätig ist, insbes. auch mit ausländischen Produktionsgesellschaften; in welcher Organisationsform es sich befindet und vor allem welche Unternehmenskultur vorherrscht. Die nachfolgende Darstellung orientiert sich an einem Unternehmen mit Produktion und Vertrieb im Inland und in ausländischen Tochtergesellschaften.⁴ Für Unternehmen, die an öffentlichen Ausschreibungen teilnehmen, wird die Einführung einer Compliance-Organisation über die Vorschriften zur Selbstreinigung nach §§ 123–125 GWB auch in Deutschland nahegelegt.
- 5 Die Beschreibung der Einführung einer Compliance-Organisation ist aus der Praxis entwickelt und verfolgt den Ansatz, auf möglichst viele Situationen übertragbar zu sein. Allerdings gibt es Grenzen. Stark regulierte Bereich wie Banken, große börsennotierte Unternehmen, insbes., wenn sie im Ausland tätig oder sogar in den USA börsennotiert sind, haben eigenständige Anforderungen an ihre Compliance-Organisation.⁵ Umgekehrt

¹ Zur Bedeutung von Compliance bei M&A-Vorgängen, vgl. Moosmayer Compliance § 4 Rn. 262–269.

² Zur Bedeutung von Compliance in der Lieferkette, vgl. Moosmayer Compliance § 4 Rn. 254–261.

³ Vgl. hierzu Moosmayer/Lösler Corporate Compliance/Lösler § 1 Rn. 30; Moosmayer/Lösler Corporate Compliance/Klahold/Lochen § 13 Rn. 4,5.

⁴ Der Autor ist in der B. Braun Melsungen SE tätig. Der Konzern hat ca. 63 000 Mitarbeiter 8,755 Mrd. EUR Umsatz (Stand: 31.12.2023) und ist in mehr als 50 Landesgesellschaften viele davon mit eigener Produktion aktiv. Es handelt sich um eine familiengeführte Europäische Aktiengesellschaft.

⁵ Allg. Moosmayer/Lösler Corporate Compliance/Lösler § 1 Rn. 4 und Moosmayer/Lösler Corporate Compliance/Klahold/Lochen § 13 Rn. 35–38. Zu nennen sind hier insbes. der Foreign Corrupt Practices Act